Monitor SD-Routing Devices

First Published: 2024-03-28

Last Modified: 2024-08-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

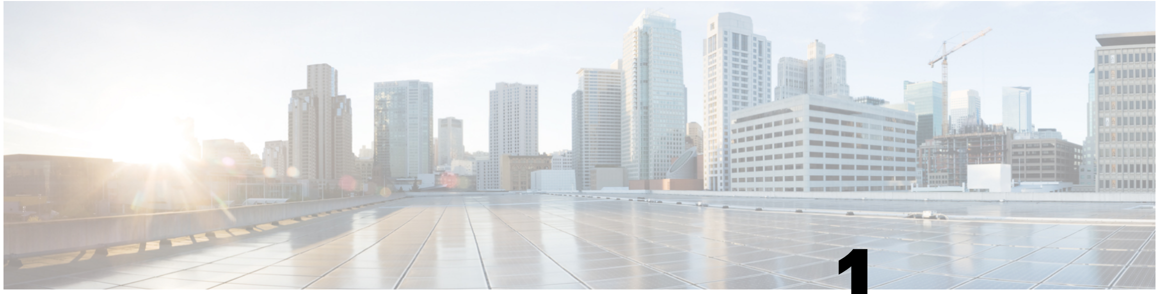
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



CHAPTER 1

Application Performance Monitoring on SD-Routing Devices

This chapter includes information on how to monitor application performance on SD-Routing devices. It contains the following sections:

Reference the Chapter Map here

Information about Application Performance Monitor

The Application Performance Monitor feature is a simplified framework that enables you to configure intent-based performance monitors. With this feature, you can view real-time, end-to-end application performance filtered by client segments, network segments, and server segments. This information helps you optimize application performance.

An application performance monitor is a predefined configuration that is used to collect performance metrics for specific traffic.

Key Concepts in Application Performance Monitoring

- **Monitoring Profile:** A profile is a predefined set of traffic monitors that can be enabled or disabled for a context. As part of this feature, the SD-Routing performance profile include Application Response Time (ART) aggregation monitor to monitor traffic passing through Cisco Catalyst SD-Routing interfaces. The SD-Routing performance profile has a dedicated policy to filter traffic based on your intent.

- **Context:** A context represents a performance monitor policy map that is attached to an interface for ingress and egress traffic. A context contains information about a traffic monitor that has to be enabled. When a context is attached to an interface, two policy-maps are created, one each for ingress and egress traffic. Depending on the direction specified in the traffic monitor, the policy maps are attached in that direction and the traffic is monitored.

Application Performance Monitor Workflow

You can enable performance monitor only on Direct Internet Access (DIA) interfaces. Performance is monitored for traffic going out of, and coming into the DIA interfaces. You can then view details of the application that you are monitoring using various show commands.

Prerequisites for Application Performance Monitoring

- Minimum software version for Cisco IOS XE Catalyst SD-Routing devices: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Limitations

The limitations for Application Performance Monitor are:

- The Application Performance Monitor support only ART on the SD-Routing device.
- Only Direct Internet Access (DIA) scenario is supported in this release
- Performance monitoring is only supported on IPv4 traffic. IPv6 traffic is not supported.
- Application Performance Monitor does not support multi application-aggregation monitors on the device.
- The class-map used in APM only supports maximum two layer class-map and does not support three or more layer class-map.
- Only CLI based config group is supported on Cisco SD-WAN Manager to config APM for SD-Routing device.

Configuring Application Performance Monitor

You can enable application performance monitor on DIA interfaces and monitor the traffic metrics for ART.

Enabling Performance on DIA Interface

The following example shows how to configure a performance monitor context using the SD-Routing application-aggregation profile. This configuration enables monitoring of traffic metrics for ART and applies it to a specific interface.

```
class-map match-any APP_PERF_MONITOR_APPS_0
 match protocol attribute application-group amazon-group
 match protocol attribute application-group box-group
 match protocol attribute application-group concur-group
 match protocol attribute application-group dropbox-group
 match protocol attribute application-group google-group
 match protocol attribute application-group gotomeeting-group
 match protocol attribute application-group intuit-group
 match protocol attribute application-group ms-cloud-group
 match protocol attribute application-group oracle-group
 match protocol attribute application-group salesforce-group
 match protocol attribute application-group sugar-crm-group
 match protocol attribute application-group webex-group
 match protocol attribute application-group zendesk-group
 match protocol attribute application-group zoho-crm-group
class-map match-any APP_PERF_MONITOR_FILTERS     --- class-map max 2 layer supported, 3 or
 more layer class-map not supported for APM feature
 match class-map APP_PERF_MONITOR_APPS_0
!
```

This configuration example shows how to configure the context of performance monitor.

```
performance monitor context APP_PM_POLICY profile application-aggregation
 exporter destination local-controller source Null0
 traffic-monitor art-aggregated class-and APP_PERF_MONITOR_FILTERS interval-timeout 300
sampling-interval 100
```

This configuration example shows how to enable the performance monitor context on an interface.

```
interface GigabitEthernet1                                                   --- DIA
interface(s)
 performance monitor context APP_PM_POLICY
```

Configuring Application Performance Monitoring on SD-Routing Device

To create a configuration group, perform these steps:

Step 1 From Cisco IOS XE Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Add CLI based Configuration Group** .

Step 2 In the **Add CLI based Configuration Group** pop-up dialog box, enter the configuration group name.

Step 3 Click the **Solution Type** drop-down list and select the solution type as **sd-routing** for the SD-Routing devices.

Step 4 In the **Description** field, enter a description for the feature

Step 5 Click **Next**.

Step 6 Click the **Load Running Config from Reachable Device** drop-down list and select the running configuration or add the configuration CLI in text box.

Step 7 Click **Save**

Step 8 Click **…** adjacent to the configuration group name and choose **Edit**

Step 9 Click **Associated Devices**.

Step 10 Choose one or more devices, and then click **Deploy**

Note Application Performance Monitoring does not support performance monitor context profile and flow monitor change when the performance monitor context profile and flow monitor are attached to an interface.

Step 11 Click **Configuration** > **Configuration Groups** > **Deploy**

Step 12 Click **…** adjacent to the configuration group name and choose **Edit** to modify performance monitor context profile and flow monitor and re-attach it to the interface.

Step 13 Click **Deploy**.

Step 14 Click **Save**.

Verifying Application Performance Monitor

To verify the Application Performance Monitor configuration on the SD-Routing device , use the **show performance monitor cache monitor** command.

```
Device#show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record
Monitor: APP_PM_POLICY-art_agg
```

```
Data Collection Monitor:
  CAT-art-aggregated CTX:0 ID:2947958679|2000002 Epoch:0
  Max number of records:             675000
  Current record count:              7
  High Watermark:                    13
  Record added:                      14
  Record aged:                       7
  Record failed to add:              0
  Synchronized timeout (secs):       300


FLOW DIRECTION:                         Output
TIMESTAMP MONITOR START:                14:10:00.000
FLOW OBSPOINT ID:                       4294967298
INTERFACE OVERLAY SESSION ID OUTPUT:    0
IP VPN ID:                              65535
APPLICATION NAME:                       layer7 share-point
connection server resp counter:         1477
connection to server netw delay sum:    10822  < --- SND_ samples
connection to server netw delay min:    100
connection to server netw delay max:    103
connection to client netw delay sum:    3559 < --- CND_ samples
connection to client netw delay min:    20
connection to client netw delay max:    198
connection application delay sum:      936
connection application delay min:      0
connection application delay max:      122
connection responder retrans packets:   2    <---- lost_samples
connection to server netw jitter mean:  0
connection count new:                   108      < ---- SND/CND_counts
connection server packets counter:      2018     <---- total_samples

Latency(SND  ms) = SND_ samples/ SND/CND_counts
Latency(CND  ms) = CND_ samples/ SND/CND_counts
Loss ratio = lost_samples /total_samples
```

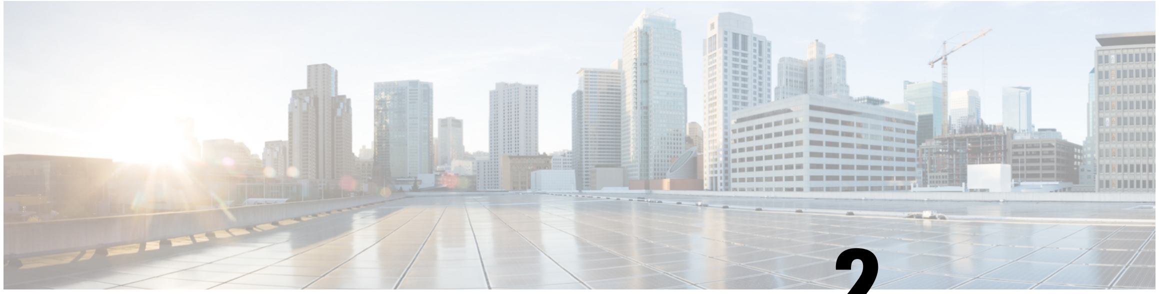
Feature Information for Application Performance Monitor

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for Application Performance Monitor

Feature Name	Releases	Feature Information
Cisco SD-Routing Application Performance Monitor	Cisco IOS XE Release 17.13.1a	The Application Performance Monitor feature introduces a simplified framework that enables you to configure intent-based performance monitors. With this framework, you can view real-time, end-to-end application performance filtered by client segments, network segments, and network segments.



CHAPTER 2

Flexible NetFlow Application Visibility on SD-Routing Devices

This chapter includes information on how to configure Flexible NetFlow Application Visibility on SD-Routing devices. It contains the following sections:

Information About Flexible Netflow Application Visibility

The Flexible NetFlow (FNF) provides statistics on packets flowing through the device. The FNF on WAN or LAN interfaces provide visibility for all the traffic (both ingress and egress) hitting the WAN or LAN interfaces on Cisco SD-Routing devices by using the Application Intelligence Engine (SAIE). The Application Intelligence Engine flow provides the ability to look into the packet past the basic header information. The SAIE flow determines the contents of a particular packet, and then either records that information for statistical purposes or performs an action on the packet.

Note You can apply FNF only on WAN or LAN interfaces. You should not apply on both WAN and LAN interfaces.

To enable t he Flexible Netflow Application Visibility on the device, you must enable the flow data aggregation using Cisco SD-WAN Manager in the following ways:

- Performance monitor context profile (recommended method)
- Flow exporter to local controller

Note If you have a existed FNF monitors, to avoid performance impact by adding a new performance monitor, add the flow exporter to local controller as flow exporter of existed FNF monitor. Otherwise, you can use the performance monitor context profile.

Prerequisites for Flexible NetFlow Application Visibility with SAIE Flows

The following are the prerequisites:

- Ensure that the device run the Cisco IOS XE 17.13.1a image.
- Ensure that you enable flow data aggregation in Cisco SD-WAN Manager.

Limitations

The following are the limitations:

- Only Aggregated statistics by Cisco SD-WAN Application Intelligence Engine (SAIE) is suppotted.
- On-demand troubleshooting is not supported.
- If context profile and FNF exporter uses the same name, the **show flow exporter name** command will display only one of them.
- The performance monitor context profile and flow exporter to local controller can only use either the context profile or flow exporter to local controller. Otherwise, it will dobule count the packets.
- Only CLI based configuration group is supported.

Enabling Flexible NetFlow Application Visibility

You can enahle the FNF Application Visibility either using the context profile or flow exporter on the device.

Configuring Context Profile Option-1

It is recommended to use this option. This example shows how to enable flow data aggregation using Context Profile on the device:

```
performance monitor context FNF profile app-visibility
 exporter destination local-controller source Null0
 traffic-monitor app-visibility-stats

interface GigabitEthernet5
 performance monitor context FNF
```

Device will apply this profile to FNF flow monitor when it is attached to an interface.

Configuring Flow Exporter Option-2

This example shows how to enable flow data aggregation using Flow Exporter on the device:

```
flow exporter fnf-1
 destination local controller
 export-protocol ipfix
 template data timeout 300
 option interface-table timeout 300
 option vrf-table timeout 300
 option application-table timeout 300
 option application-attributes timeout 300

flow record fnf-app-visiblility
 match routing vrf input
 match interface input
 match interface output
 match application name
 collect counter bytes long
 collect counter packets long

flow monitor fnf-app-visiblility
 exporter fnf-1
 cache timeout inactive 10
 cache timeout active 60
 cache entries 5000
 record fnf-app-visiblility

interface GigabitEthernet5
 ip flow monitor fnf-app-visiblility input
 ip flow monitor fnf-app-visiblility output
 ipv6 flow monitor fnf-app-visiblility input
 ipv6 flow monitor fnf-app-visiblility output
```

Configuring Flexible NetFlow Application Visibility

To configure FNF Application Visibility, on the SD-Routing device, perform these steps:

Step 1 From Cisco IOS XE Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** > **Add CLI based Configuration Group** .

Step 2 In the **Add CLI configuration Group** pop-up dialog box, enter the configuration group name.

Step 3 Click the **Solution Type** drop-down list and select the solution type as **sd-routing** for the SD-Routing devices.

Step 4 In the **Description** field, enter a description for the feature

Step 5 Click **Next**

The new configuration group page is displayed with the Feature Profiles and Associated Device tabs.

Step 6 In the **Feature Profiles** section, add the corresponding configuration.

Step 7 Click **Save** to save the configuration.

Step 8 Click **(…)** adjacent to the configuration group name and choose **Edit**

Step 9 Click **Associated Devices**.

Step 10 Choose one or more devices, and then click **Deploy**

Note Flexible Netflow does not support performance monitor context profile and flow monitor change when the performance monitor context profile and flow monitor are attached to an interface.

Step 11 Click **Configuration** > **Configuration Groups** > **Deploy**

Step 12 Click **(…)** adjacent to the configuration group name and choose **Edit** to modify performance monitor context profile and flow monitor and re-attach it to the interface.

Step 13 Click **Deploy**.

Step 14 Click **Save**.

Verifying Flexible NetFlow Application Visibility Using Cisco SD-WAN Manager

To verify the FNF Application Visibility, perform the following steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select a SD-Routing device from the list.

Step 2 In the left pane, choose **SAIE Applications**> **Fliter**.

Step 3 In the **Filter By** dialog box, select the VPN.

Step 4 For the Traffic Source, check either the **LAN** or **Remote Access** check box.

Step 5 Click **Search** to search the flow records based on the selected filters.

The flow records are displayed.

Step 6 Click **Export** to export the flow records to your local system.

Step 7 Click **Reset All** to reset all the search filters.

Verifying Flexible NetFlow Application Visibility

To check the basic network metrics that are used to calculate the the SD-Routing FNF application visibility, use the **show performance monitor context** [profile name] **configuration**, **show platform sofware td-l database content dta fnf-statistics**, and **show performance monitor context fnf traffic monitoring app-visibility-stats cache** commands.

```
Device #show performance monitor context fnf configuration
!===============================================================================
! Equivalent Configuration of Context fnf !
!===============================================================================
!Exporters
!==========
!
flow exporter fnf-1
description performance monitor context fnf exporter
destination local controller
export-protocol ipfix
template data timeout 300
option interface-table timeout 300 export-spread 0
option vrf-table timeout 300 export-spread 0
option application-table timeout 300 export-spread 0
option application-attributes timeout 300 export-spread 0
!
!Access Lists
!=============
!Class-maps
!===========
!Samplers
!=========
!Records and Monitors
!=====================
!
flow record fnf-app-visiblility-v4
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v4
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visiblility-v4
!
!
flow record fnf-app-visiblility-v6
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v6
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visiblility-v6
!
!Interface Attachments
!======================
interface GigabitEthernet5
ip flow monitor fnf-app-visiblility-v4 input
ip flow monitor fnf-app-visiblility-v4 output
ipv6 flow monitor fnf-app-visiblility-v6 input
ipv6 flow monitor fnf-app-visiblility-v6 output
```

```
Device# show performance context fnf traffic-monitor app-visibility stats cache
Monitor fnf-app-visibility-v4

Cache  type:                           Normal (platform cache)
Cache  size :                                10000
Current entries:                              2
High Watermark:                               4

Flows added:                                  6
Flows aged:                                   4
 - Inactive timeout           (10sec)         4

IP VRF  ID INPUT  INFE INPUT  INTF OUTPUT  APP Name           bytese long   pkts long
```

```
======  =======   =========   ===========  ===============    ===========  ==========
1         (1)       Gi3         Gi5        layer7 share-point  1517476       3277
1         (1)       Gi5         Gi3       layer7 share-point  1306568       3463
```

Feature Information for Flexible NetFlow Application Visibility on SD-Routing Devices

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 2: Feature Information for Flexible NetFlow Application Visibility on SD-Routing Devices

Feature Name	Releases	Feature Information
Flexible NetFlow Application Visibility on SD-Routing Devices	Cisco IOS XE Release 17.13.1a	The Flexible NetFlow (FNF) feature provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Also, it provides visibility for all the traffic that passes through the VPN0 on Cisco SD-Routing devices by using the SD-Routing Application Intelligence Engine (SAIE).

CHAPTER 3

Flow Level Flexible NetFlow Support for SD-Routing Devices

This chapter includes information on how to configure Flow Level Flexible NetFlow Support for SD-Routing devices. It contains the following sections:

Information on Flow Level Flexible NetFlow

Flexible NetFlow is an advancement on the original NetFlow that adds the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

The Security Unified Logging (SUL) profile acts as a superset containing all the information present in an application-level and a flow-level profile.

If you do not require detailed flow-level statistics, you can use Application Visibility for your FNF monitors. Alternatively, you can enable the flow-level FNF monitor to view all the data that is captured including application-level statistics.

By enabling flow-level visibility monitor on either the LAN interface or WAN interface, you can avoid double packet counts. This prevents data redundancy which is caused by ingress and egress data traffic flow from LAN to WAN.

The IPv4 and the IPv6 protocols are enabled by default after the performance monitor context is attached to an interface. But, you can choose to enable either IPv4 or IPv6 protocols by configuring the performance monitoring context.

Types of Flexible NetFlow Monitoring for SD-Routing Devices

SD-Routing supports three types of FNF monitoring methods:

- Aggregated NetFlow Application Visibility
- Flow-level FNF
- Security Unified Logging (SUL)

Benefits of Flow-level Flexible NetFlow

Following are the benefits if you enable Flow-level FNF:

- Flow-level FNF provides statistics at a granular level.
- Flow-level FNF statistics are used in Cisco Catalyst SD-WAN Analytics and SD-WAN monitoring for On-demand troubleshooting.

Flow-level Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform data export and traffic analysis. The user-defined flow records and the component structure of Flexible NetFlow facilitates the creation of various configurations for exporting the data and analysing traffic on a networking device with a minimum number of configuration commands.

Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The following sections provide more information on Flexible NetFlow components:

- **Flow Records**

  In Flexible NetFlow a combination of key and nonkey fields is called a record. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data.

- **Flow Exporters**

  Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

- **Flow Monitors**

Flow monitors are the Flexible NetFlow components which are applied to interfaces to perform network traffic monitoring.

Flow monitors consist of a user-defined record, an optional flow exporter, and a cache that is automatically created at the time the flow monitor is applied to the first interface.

Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record.

Ways to Enable Flexible NetFlow Monitors on SD-Routing Devices

There are two ways to enable Flow-level FNF:

- **Using an EzPM Profile**: This is a simple recommended way where you can use the existing profiles to configure flow records. By using EzPM profile, you can configure Application-visibility, Flow-level visibility, and SUL monitors.
- **Using a Flow Monitor**: This is a manual process where flow records are created and exported to a Local Exporter for Application-visibility, Flow-level visibility, and SUL.

Prerequisites to Configure Flow-level Flexible NetFlow

You need to enable license boot-level advantage on the Cisco router. This gives you the network advantage to use EzPM profile CLI support.

Limitations to Configure Flow-level Flexible NetFlow

Following are the limitations on configuring flow-level FNF:

- Flow-level configuration for SD-Routing devices is possible on the Cisco SD-WAN Manager through CLI based configuration groups, CLI templates, or CLI Add-on profiles.
- Application-level and Flow-level visibility monitors both ingress and egress data on the target interface. If configured on both service and transport interface, the packet for the same flow is counted twice.
- Customizing flow monitors with partial flow-level record fields is not allowed. If partial flow-level record fields are added to monitors, PSV data is not generated.
- You can configure either application-visibility, flow-level, or the SUL profile on one interface. You can attach only one type of EzPM profile to an interface.

Configure Flow-level FNF on an SD-Routing Device using EzPM Profile

To enable Flow-level FNF monitoring, you can use the default Easy Performance Monitor (EzPM) profile. You can read more about EzPM here.

Flow-level visibility contains both application-level statistics and flow-level statistics. This eliminates the need to enable application-level visibility for your FNF monitors.

Step 1 Create an EzPM profile.

```
Device# configure terminal
Device(config)# performance monitor context context_name profile flow-level-visibility
Device(config-perf-mon)# exporter destination local-controller source Null0
Device(config-perf-mon)# traffic-monitor flow-level-visibility-stats
Device(config-perf-mon)# end

Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

Step 2 Apply performance monitor context to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

Configure Flow-level Flexible NetFlow using a Flow Monitor

To configure flow-level FNF using a flow monitor, perform the following steps:

Step 1 Create a FNF flow exporter to configure flow records.

```
Device# configure terminal
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout seconds
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# exit
```

Step 2 Create a flow record for the flow-level view for IPv4 traffic.

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 3 Create a flow record for the flow-level view for IPv6 traffic.

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv6
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv6 destination address
Device(config-flow-record)# match ipv6 protocol
Device(config-flow-record)# match ipv6 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv6 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 4 Enable a flow monitor to perform network traffic flow-level visibility for IPv4 traffic.

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visiblility-v4
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv4
Device(config-flow-monitor)# end
```

Step 5 Enable a flow monitor to perform network traffic flow-level visibility for IPv6 traffic.

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visiblility-v6
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv6
Device(config-flow-monitor)# end
```

Step 6 Apply the flow monitor to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor fnf-flow-level-visiblility-v4 input
Device(config-if)# ip flow monitor fnf-flow-level-visiblility-v4 output
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-v6 input
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-v6 output
Device(config-if)# end
```

What to do next

Monitor Flow-level Data on the SD-Routing Device

Information on Security Unified Logging

Security Unified Logging allows you to have visibility into the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP. These features help you to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol, or applications.

SUL profiles have all the flow-level fields in it, so you do not need to attach flow-level visibility to an interface if the SUL profile is already attached to it. SUL supports both IPv4 and IPv6 protocols.

Limitations to Configure Security Unified Logging on a Device

Following are the limitations to configure SUL on a device:

- The SUL profile should not be configured if other FNF profiles are configured, such as application-visibility (aggregate FNF) or flow-visibility. These three profiles should be mutually exclusive to avoid data redundancy.
- Customizing flow monitors with partial SUL record fields is not allowed. If partial SUL record fields are added to monitors, PSV data is not generated.
- Due to a design limitation, by default, SUL needs to be applied to both LAN and WAN interface since SUL monitor only collects the output direction.

Configure Security Unified Logging on an SD-Routing Device using an EzPM Profile

There are two ways defined below to configure SUL on an SD-Routing device.

Step 1 Configure an EzPM profile.

```
Device# configure terminal
Device(config)# performance monitor context context_name profile security-unified-logging
Device(config-perf-mon)# exporter destination local-controller source Null0
Device(config-perf-mon)# traffic-monitor sul-fnf-config
Device(config-perf-mon)# end
```

Step 2 Apply the performance monitor context to the interface.

```
Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

What to do next

Monitor Security Unified Logging Data on the SD-Routing Device

Configure Security Unified Logging on an SD-Routing Device using Flow Monitor

To configure SUL using a flow monitor, perform the following steps:

SUMMARY STEPS

1. Create a flow exporter for SUL.
2. Configure the flow records.
3. Enable a flow monitor for SUL.
4. Apply the flow monitor to the interface.

DETAILED STEPS

Step 1 Create a flow exporter for SUL.

```
Device# configure terminal
Device(config)# flow exporter sul-1
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option utd-category-table
Device(config-flow-exporter)# option utd-file-type-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# option c3pl-class-table
Device(config-flow-exporter)# option c3pl-policy-table
Device(config-flow-exporter)# option fw-zone-pair-table
Device(config-flow-exporter)# option fw-zone-table
Device(config-flow-exporter)# option fw-proto-table
Device(config-flow-exporter)# option utd-drop-reason-table
Device(config-flow-exporter)# option sdvt-drop-reason-table
Device(config-flow-exporter)# exit
```

Step 2 Configure the flow records.

```
Device# configure terminal
Device(config)# flow record sul-sul-monitor-v4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect ulogging fw-zp-id
Device(config-flow-record)# collect ulogging fw-zone-id-array
Device(config-flow-record)# collect ulogging fw-class-id
Device(config-flow-record)# collect ulogging fw-policy-id
Device(config-flow-record)# collect ulogging fw-proto-id
Device(config-flow-record)# collect ulogging fw-action
Device(config-flow-record)# collect ulogging fw-src-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-dst-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-src-port-translated
Device(config-flow-record)# collect ulogging fw-dst-port-translated
Device(config-flow-record)# collect ulogging utd-ips-pri
Device(config-flow-record)# collect ulogging utd-ips-sid
Device(config-flow-record)# collect ulogging utd-ips-gid
Device(config-flow-record)# collect ulogging utd-ips-cid
Device(config-flow-record)# collect ulogging utd-urlf-url-hash
Device(config-flow-record)# collect ulogging utd-urlf-url-category
Device(config-flow-record)# collect ulogging utd-urlf-url-reputation
Device(config-flow-record)# collect ulogging utd-urlf-app-name
Device(config-flow-record)# collect ulogging utd-amp-dispos
Device(config-flow-record)# collect ulogging utd-amp-filename-hash
Device(config-flow-record)# collect ulogging utd-amp-file-type
Device(config-flow-record)# collect ulogging utd-amp-file-hash
Device(config-flow-record)# collect ulogging utd-amp-malname-hash
Device(config-flow-record)# collect ulogging utd-drop-reason-id
Device(config-flow-record)# collect ulogging sdvt-drop-reason-id
Device(config-flow-record)# collect ulogging utd-ips-policy-id
Device(config-flow-record)# collect ulogging utd-ips-action-id
Device(config-flow-record)# collect ulogging utd-urlf-policy-id
Device(config-flow-record)# collect ulogging utd-urlf-action-id
Device(config-flow-record)# collect ulogging utd-amp-policy-id
Device(config-flow-record)# collect ulogging utd-amp-action-id
Device(config-flow-record)# collect ulogging utd-urlf-reason-id
Device(config-flow-record)# collect ulogging flow-direction
Device(config-flow-record)# collect ulogging fw-user-name
Device(config-flow-record)# collect ulogging fw-src-ipv6-addr-translated
Device(config-flow-record)# collect ulogging fw-dst-ipv6-addr-translated
Device(config-flow-record)# end
```

Step 3 Enable a flow monitor for SUL.

```
Device# configure terminal
Device(config)# flow monitor sul-sul-monitor-v4
Device(config-flow- monitor)# exporter sul-1
Device(config-flow- monitor)# record sul-sul-monitor-v4
Device(config-flow- monitor)# end
```

Step 4 Apply the flow monitor to the interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor sul-sul-monitor-v4 output
Device(config-if)# end
```

What to do next

Monitor Security Unified Logging Data on the SD-Routing Device

Enable Flow-level Flexible NetFlow for SD-Routing Devices

To enable flow-level FNF using Cisco SD-WAN manager, begin with creating a configuration group followed by the steps provided below.

Create a Configuration Group

To create a configuration group, perform the following steps:

Step 1 From Cisco Catalyst SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** and select the solution as **SD-Routing** from the **Solution** drop-down list.

Step 2 Click **Create Configuration Group** and in the dialog box, enter a name and description, select the CLI Configuration Group and click **Create**.

Step 3 From the **Load Running Config from Reachable Device** drop-down list, select the device.

Step 4 Once the CLI has loaded into the Config Preview section, click **Save**.

Associate a Device and Deploy the Configuration Group

To associate and deploy the configurations of the device, perform the following steps:

Step 1 Click **(…)** adjacent to the configuration group name and choose **Edit**.

Step 2 In the **Deployment** pane, click **Add**and select the device to be associated.

Step 3 Choose one or more devices, and then click **Deploy**.

Step 4 Click **Save**.

Monitor Flow-level Data on the SD-Routing Device

To view and monitor the flow-level information like destination IP, destination port, the source IP of a device, perform the following steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select a SD-Routing device from the list.

Step 2 From the left pane, choose **SAIE Applications** > **Filter**.

Step 3 In the **Filter By** dialog box, select the VPN and click **Search** to search the flow records based on the selected filters.

Step 4 Click **Export** to export the flow records to your local system.

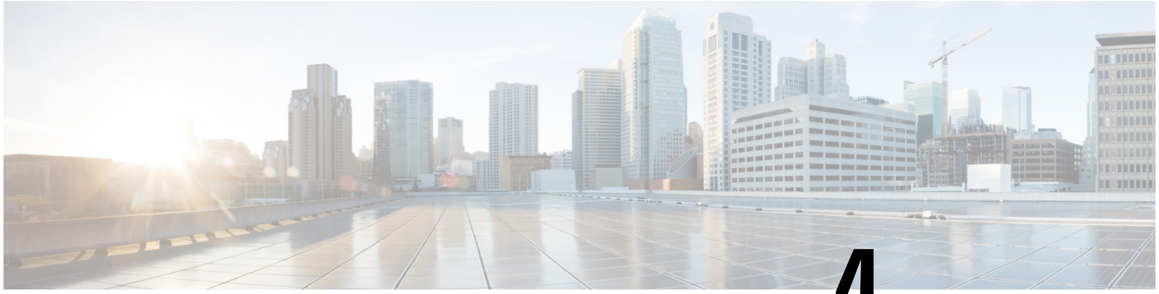
Monitor Security Unified Logging Data on the SD-Routing Device

To monitor the SUL data on the device, perform the following steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select a SD-Routing device from the list.

Step 2 From the left pane, choose **Connection Events** > **Filter**.

Step 3 In the **Filter By** dialog box, select the VPN and click **Search** to search the flow records based on the selected filters.



CHAPTER 4

Packet Capture on SD-Routing Devices

This chapter includes information on how to configure the packet capture on the SD-Routing devices. It contains the following sections:

Information about Packet Capture

The Packet Capture feature allows you to capture and analyze traffic on the SD-Routing devices. You can initiate a packet capture by selecting the target interface under the selected VRF. Also, you can set simple traffic filter by specifying the Source IP address, Destination IP address, Layer 4 protocol number and so on.

Configuring Packet Capture

Prerequisites

- Minimum software version for Cisco IOS XE Catalyst SD-Routing devices: Cisco IOS XE Catalyst SD-WAN Release 17.13.1.
- Ensure that the data stream is enabled from **Administration** > **settings** page.

Limitations

The limitations are:

- xDSL (ATM/Ethernet interface) is not supported.
- The Dynamic virtual-access interfaces are only support with FlexVPN.
- Loopback interface is not supported
- BDI and Layer 2 EFP/Service instance interfaces are not supported.

Configuring Packet Capture

To configure the packet capture, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 To choose a device, click the device name in the **Hostname** column.

Step 3 Click **Troubleshooting** in the left pane and click **Packet Capture**.

Step 4 In the **VPN** field, choose the VPN for filtering the interfaces.

Step 5 In the **Interface corresponding to the VPN**field, choose the target interface to capture the packets.

Step 6 (Optional) Click **Traffic Filters** to configure filters to capture only relevant traffic, which helps to reduces the load on the network and makes it easier to analyze specific packets.

a) In the **Source IP** field, enter the source IP address of the device to capture packet.

b) In the **Destination IP** field, enter the destination IP address of the device to capture packet.

c) In the **Source Port** field, enter the number of the source port.

d) In the **Destination Port** field, enter the number of the destination port.

Note The Source and Destination ports are applicable only when the protocol is 6 (TCP) or 17 (UDP).

e) Use the **toggle** button to enable the **Bidirectional** filter and filter both the Source IP and Destination IP traffic.

Step 7 Click **Start**.

The Cisco SD-WAN Manager starts to capture the packets with the filters specified.

Step 8 You can stop the packet capture using the **Force Stop** or using time out option. Also, when you have captured 5MB of packets, the packet capture stops automatically.

Step 9 Click the **Download** icon to download the Packet Capture file to your system.

Note Do not refresh or navigate away from the Packet Capture page during the packet capturing process is running.

Feature Information for Packet Capture for SD-Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 3: Feature Information for Packet Capture for SD-Routing

Feature Name	Releases	Feature Information
Packet Capture for SD-Routing	Cisco IOS XE Release 17.13.1a	This feature allows you to configure options to capture the bidirectional IPv6 traffic data to troubleshoot connectivity on the SD-Routing devices.

CHAPTER 5

Speed Test on SD-Routing Devices

This chapter includes information on how to configure the speed test on the SD-Routing devices. It contains the following sections:

Information About Speed Test

Internet speed test: Cisco SD-WAN Manager tests the network speed. Cisco SD-WAN Manager designates the device as the client site and the iperf3 server as the remote site. You can specify the IP address (or domain name) and port number for an iperf3 server.

The speed tests measure upload speed from the source device to the selected or specified iperf3 server, and measure download speed from the iperf3 server to the source device.

Prerequisites for Speed Test

Speed testing requires the device host name of the target device. Also, you must enable Data Stream. To enable data stream go to **Settings** page and choosing **Settings** > **Data Stream**.

Run Internet Speed Test

To run a speed test, perform the following:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following:

- **Source Interface**: From the drop-down list, choose the source interface on the local device.
- **Destination Device**: From the drop-down list, choose **Internet**.
- **iPerf3 Server**: (Optional) Enter the domain name or iPerf3 server’s IP address in IPv4 format.
- **Server Port Range**: (Optional) Enter the server port or a port range. For example, 5201, 5210, or 5201-5205.

6. Click **Start Test**.

The speed test result is displayed.

Verify Speed Test

After you successfully execute the speed test, the following details are displayed on the **Speed Test** page:

- The middle part of the right pane reports the results of the speed test.
- The clock reports the recently obtained circuit speed results.
- When measuring the uploading speed, packets are sent from the source device to the iPerf3 server, and the source device receives acknowledgments from the destination.

  When measuring the downloading speed, packets are sent from the iPerf3 server to the source device, and the destination device receives acknowledgments from the source.

Troubleshooting Speed Test Issues

The following table provides troubleshooting information for speed testing:

Table 4: Troubleshooting Scenarios

Error Information	Possible Root Cause
Failed to resolve iperf server address	DNS server is not configured at edge device or is unable to resolve the iperf server from the configured DNS server at edge device.
Speed test servers not reachable	The speed test server ping failed. The edge device cannot reach the server IP.
iPerf client: unable to connect stream: Resource temporarily unavailable	Unable to connect to the speed test server. Access may be blocked by access-control list (ACL) permissions.
iPerf client: unable to connect to server	The iPerf3 server is not providing the test service at the user-specified port or default port 5201.
Device Error: Speed test in progress	The selected source or destination device is performing a speed test and cannot start a new one.
Device error: Failed to read server configuration	The data stream configuration is missing. Workaround: Running a CLI command at the SD-Routing device and clearing the SD-Rounting control connections can fix the issue.

Error Information	Possible Root Cause
Speed test session has timed out	The speed test has not successfully completed in 180 seconds. This might be because the SD-Rouring device has lost the control connection to Cisco SD-WAN Manager during the speed testing.

Feature Information for Speed Test on SD-Routing Devices Using Cisco SD-WAN Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 5: Feature Information for Speed Test on SD-Routing Devices Using Cisco SD-WAN Manager

Feature Name	Release Information	Description
Speed Test	Cisco IOS XE 17.13.1	Cisco SD-WAN Manager allows you to measure the network speed and available bandwidth between a device and an iPerf3 server. The speed tests measure upload and download speed from the source device to the destination device.